

| [NODIS Library](#) | [Organization and Administration\(1000s\)](#) | [Search](#) |



NASA Policy Directive

NPD 1600.4

Effective Date: July 25, 2011
Expiration Date: July 25, 2016

COMPLIANCE IS MANDATORY[Printable Format \(PDF\)](#)

Request Notification of Change

(NASA Only)

Subject: National Security Programs

Responsible Office: Office of Protective Services

1. POLICY

a. NASA policy shall define security responsibilities on the oversight and management of all national security programs within NASA. This encompasses Special Access Programs (SAPs) and Sensitive Compartmented Information (SCI), to include all national security programs managed by NASA supporting the Department of Defense (DoD), the Department of Homeland Security (DHS), and the U.S. intelligence community.

b. It is NASA's policy to ensure all risk assumed by NASA to protect national security programs is coordinated with the appropriate offices. This directive establishes and identifies the security responsibilities and functions of the NASA Special Access Program Central Official (SAPCO) and the NASA Office of Protective Services (OPS) and its role as appointed by the NASA Administrator for ensuring the protection of national security programs security policy.

2. APPLICABILITY

a. This NPD is applicable to NASA Headquarters and NASA Centers, including Component Facilities and Technical and Service Support Centers.

b. This NPD applies to the Jet Propulsion Laboratory, contractors, grant recipients, consultants, or parties to agreements to the extent specified or referenced in the appropriate contracts, grants, or agreements.

c. U.S. Government agencies whose personnel require access to national security programs relating to NASA are subject to this NPD.

3. AUTHORITY

- a. National Aeronautics and Space Act of 1958, as amended, 42 U.S.C. 2455, Section 304.
- b. National Aeronautics and Space Act of 1958, as amended, 42 U.S.C. 2473 (c), Section 203 (c).
- c. Classified National Security Information, Exec. Order No. 13,526, 3 C.F.R. 298 (2009).

4. APPLICABLE DOCUMENTS

None.

5. RESPONSIBILITY

- a. Only the Administrator or designee shall:

- (1) Render the final decision on proposals to establish or terminate NASA national security programs, alter the scope of any approved national security program activity, and use NASA resources to support DoD, DHS, or national security program intelligence activities.
- (2) Establish and commit NASA to protecting national security programs.
- (3) Establish and oversee the development of security policy, requirements, and guidance for SAP and SCI national security activities.
- (4) Appoint responsible individuals for all national security program activities. The appointed individuals serve as the primary point of contact with Congress, the agencies of the Executive Branch, and intelligence agencies on all issues relating to national security programs.

- b. The Assistant Administrator (AA) for Protective Services shall:

- (1) Develop, coordinate, and promulgate all NASA national security program policies.
- (2) Perform security oversight of NASA components managing national security program assets in accordance with established security policies and guidance.
- (3) Ensure national security programs' security policies are integrated into and consistent with the development of NASA mission needs, national security and defense strategies, technology development, implementation, and operations (including contingency operations).
- (4) Oversee and, if necessary, direct credentialed counterintelligence personnel in the investigation of security violations, infractions, or counterintelligence matters regarding NASA's national security programs. Actions of this nature will be coordinated with the NASA OIG per established protocols.
- (5) Ensure a sufficient cadre of SAP and SCI trained personnel perform Agency-unique tasks associated with national security programs.
- (6) Maintain responsibility for sufficient resources to provide the security needs defined in this directive and other interagency security agreements.

(7) Review all national security program risks, mitigate these risks where applicable, and provide a risk assessment of the Agency's national security programs to the NASA Administrator or designee.

(8) Submit reporting of national security information (NSI) within NASA program activities to Congress.

c. The NASA SAP Coordination Official (SAPCO) and SCI Program Manager support the NASA Administrator in carrying out security oversight and management responsibilities for NSI.

1) The NASA SAPCO shall:

(a) Serve as the principal security point of contact in NASA for all SAP security requirements.

(b) Act as the NASA security liaison for all DoD and intelligence SAPs.

(c) Participate in security planning for new projects and testing activities.

(d) Provide security oversight and guidance to SAP managers within NASA.

(e) Develop, coordinate, and publish NASA SAP security management policy, instructions, and publications.

(f) Develop, coordinate, promulgate, and oversee the implementation of special security countermeasures policy, including those associated with arms control and nonproliferation initiatives that could impact DoD- sensitive equities.

(g) Submit SAP establishment requests to the Office of the President through the National Security Council and coordinate new activities with the DoD Under Secretary of Defense for Acquisition, Technology, and Logistics.

(h) Develop and maintain a partnership with the program management, providing security cost, risk analysis of the program security posture, and security guidance to NASA program managers.

(i) Process program security documents required for approval, validate annual program security requirements, and oversee a security inspection and compliance program.

(j) Report cases of fraud, waste, and/or abuse of SAP resources to the appropriate authorities and to the Office of the Inspector General.

(2) The NASA SCI Program Manager shall:

(a) Serve as the principal point of contact in NASA for all SCI requirements.

(b) Act as the NASA liaison for all SCI.

(c) Participate in the budget and program reviews for SCI.

(d) Provide security oversight and guidance to SCI managers within NASA.

(e) Develop, coordinate, and publish SCI security policy, instructions, and publications.

(f) Develop, coordinate, promulgate, and oversee the implementation of Special Security Policy.

(g) Process program security documents required for approval, validate annual program security requirements, and oversee a security inspection and compliance program.

d. NASA Center Directors, Center Chiefs of Security, and Mission Directors must ensure appropriate coordination has been made with the OPS regarding the type of classified information, the classification level, and scope of program.

6. DELEGATION OF AUTHORITY

- a. The NASA Administrator may redelegate his authority as identified in this NPD.
- b. Each delegation will identify a specific individual to serve as the designee for the positions identified Sections in 5.a and 5.c of this NPD.
- c. The delegation of authority shall not be redelegated further without the approval of the NASA Administrator.
- d. The SAPCO authority may be delegated to a subordinate official. Such a delegation will identify, by name and position title, the subordinate official and the specific authority that is being delegated. Any further delegation of authority must be approved by the SAPCO and must also identify, by name and position title, the subordinate official.

7. MEASUREMENTS

None.

8. CANCELLATION

None.

**/s/ Charles F. Bolden, Jr.
Administrator**

ATTACHMENT A: (TEXT)

ATTACHMENT A: REFERENCES

A.1 Access to Classified Information Procedures, 50 U.S.C. 435.

A.2 Reforming Processes Related to Suitability for Government Employment, Fitness for Contractor Employees, and Eligibility for Access to Classified National Security Information, Exec. Order No. 13,467 (2008).

A.3 NASA Procedural Requirement 1600.1, Security Program Procedural Requirements.

A.4 NASA Special Access Program Security Guide.

ATTACHMENT B: DEFINITION OF KEY TERMS

B.1 Sensitive Compartmented Information (SCI) - Classification level denoting information, generally intelligence related, requiring security clearances and physical/procedural security measures above those established for collateral classified information or SAP information.

B.2 Special Access Programs (SAP) - Any program established and approved under EO 12958 that imposes need-to-know or access controls beyond those normally required for access to collateral Confidential, Secret, or Top Secret information.

**/s/ Charles F. Bolden, Jr.
Administrator**

(URL for Graphic)

**DISTRIBUTION:
NODIS**

This Document Is Uncontrolled When Printed.

Check the NASA Online Directives Information System (NODIS) Library to Verify that this is the correct version before use: <http://nodis3.gsfc.nasa.gov>
